

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

☒ FILED ☐ ENTERED
☐ LOGGED ☐ RECEIVED
 12:28 pm, Dec 15 2022
 AT BALTIMORE
 CLERK, U.S. DISTRICT COURT
 DISTRICT OF MARYLAND
 BY _____ Deputy

IN THE MATTER OF:

**1) CRIMINAL COMPLAINT AND
ARREST WARRANT FOR EDNA
LENORE DINEEN LOPEZ**

FILED UNDER SEAL

CASE NO. 22-mj-3656-MJM

2) THE SEARCH OF:

**a. THE PREMISES LOCATED
AT 1528 MOUNTMOR CT,
BALTIMORE, MD 21217**

Misc. No. 22-mj-3657-MJM
22-mj-3658-MJM

**b. THE PERSON OF EDNA
LENORE DINEEN LOPEZ**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Rachal M. Torg, a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

1. I have been employed as an HSI Special Agent since November 2017. As part of the daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, U.S.C. §§ 2251, 2252 and 2252A. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received formal training through HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material, and internet crime. I have participated in the execution of numerous search warrants, of which the majority has involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United

States Code § 2252A involving child exploitation offenses. In the course of my employment with HSI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This Court has jurisdiction to issue the requested search warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The procedure by which the government will search and seize the information contained is described in Attachments A and B, which are incorporated by reference.

PURPOSE OF THIS AFFIDAVIT

4. I make this affidavit in support of application for:
- a. A criminal complaint and arrest warrant charging **EDNA LENORE DINEEN LOPEZ** with 18 U.S.C. 2251(a)(Sexual Exploitation of Children); 18 U.S.C. 2252A(a)(2) Distribution of Child Pornography; and 18 U.S.C. 1591 (a), (b)(1)(Sex Trafficking of Children).
 - b. A search warrant under Rule 41 of the Federal Rules of Criminal Procedure to search:
 - i.) The entire premises located at **1528 Mountmor Ct, Baltimore, Maryland, 21217 (SUBJECT PREMISES)**, more specifically described in Attachment A-1, which is incorporated herein by reference;
 - ii.) The person of **Edna Lenore Dineen LOPEZ (“LOPEZ”)**, more specifically described in Attachment A-2, which is incorporated herein by reference;

5. The **SUBJECT PREMISES** and **LOPEZ** described above in sections i. and ii. are collectively referred to as the “**TARGET LOCATIONS**” in this affidavit.

6. The purpose of this application is to seize evidence of violations of 18 U.S.C. § 2251(a) (Sexual Exploitation of Children); 18 U.S.C. § 2252A(a)(2) (Distribution of Child Pornography); 18 U.S.C. § 1591(a),(b)(1) (Sex Trafficking of Children); and 18 U.S.C. § 2252A(a)(5)(B) (Possession of Child Pornography) (collectively the “**TARGET OFFENSES**”).

7. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of the **TARGET OFFENSES** are located within the **TARGET LOCATIONS**.

SUMMARY CONCERNING CHILD SEX TRAFFICKING, CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT, AND/OR PRODUCE CHILD PORNOGRAPHY, AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT, DISTRIBUTION, AND PRODUCTION OF CHILD PORNOGRAPHY

8. Based upon my training and experience in child sexual exploitation, child sex trafficking, and child pornography investigations, and having worked with other experienced law enforcement officers in child exploitation investigations, I know the following:

a. Persons who have a sexual interest in children or are involved with child pornography generally also have other sexually explicit materials related to their interest in children, which may consist of photographs, motion pictures, videos, text material, computer graphics and digital or other images of children. Such persons may also have images of children or text writing that do not rise to the level of child pornography but nonetheless fuel their deviant sexual fantasies involving minors. Such persons have been known to take and maintain photographs and video recordings of fully clothed children, not just in sexually provocative poses, but in public places and elsewhere. I am aware that this sort of material has been admitted in trials

under Fed.R.Evid. 404(b) to prove such things as the possessor's knowledge, intent, motive, and identity, and under Fed.R.Evid. 414 to prove the person has a sexual interest in minors.

b. Individuals who have a sexual interest in children or images of children as described above and child pornography often maintain these images on cameras, film, video cameras, videos, computers, and other photographic equipment. Such individuals have been known to connect their cameras, video cameras, and other photographic equipment to their computers in an effort to create added storage space for their images of children.

c. Individuals who have a sexual interest in children or collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. They do this to gain status, trust, acceptance, and support and to increase their collection of illicit images and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, chat and file sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat ("IRC"), newsgroups, Internet clubs, and various forms of Instant Messaging such as Yahoo! Messaging, and "chat" that is sometimes saved on the users' computer or other digital storage media.

d. Besides photos of minors and child erotica, such individuals often produce and/or collect other written material on the subject of sexual activities with minors, which range from fantasy stories to medical, sociological, and psychological writings, which they save to understand and justify their illicit behavior and desires.

e. Individuals who have a sexual interest in children or collect child pornography often collect, read, copy, or maintain names, addresses, including e-mail addresses, phone numbers, and lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests, or have child pornography and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or, sometimes, commercial profit. They may maintain these names on computer storage devices, web sites or other Internet addresses, and their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of child pornography.

f. Individuals who have a sexual interest in children or collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures. These individuals may also protect their illicit materials by saving it on movable media such as memory cards, memory sticks, CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or sent to third party image storage sites via the Internet.

9. Based on my investigative experience related to computer and internet related child sex trafficking and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. Computers and computer technology have also revolutionized the way in which child sex traffickers are able to interact with consumers of commercial sex acts and use and exploit children as the victims of commercial sex acts. The ability to surreptitiously advertise, solicit, recruit, or entice children for commercial sex has caused the market for child sex trafficking to increase exponentially as less resources are needed to reach consumers and groom and recruit children. Relatedly, the ability to transfer money or other currency without having to interact in person has increased the anonymity of commercial sex consumers and traffickers as well as allowed for commercial sex acts to be committed in a voyeuristic way instead of direct contact.

c. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors and child sex traffickers to interact with and sexually exploit children. Computers, smartphones, and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

d. Mobile devices such as laptop computers, smartphones, iPods, iPads, and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

e. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, and can also send and receive money for commercial sex, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

f. Gaming systems, such as PlayStation and XBOX platforms have similar attributes as computer devices. Gaming systems can contain hard drives and store data as well as access the Internet using web browsers. Gaming system also have the ability to communicate through messaging and chats, similar to computers.

g. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

h. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

i. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

j. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

k. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the **TARGET LOCATIONS**, notwithstanding the passage of time.

l. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

m. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

n. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

o. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

p. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

10. Based on traits shared by collectors, the use of e-mail, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the sex trafficking of children, as well as the production, distribution, receipt, and possession of child pornography will be found in the **TARGET LOCATIONS**, notwithstanding the passage of time.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS AND/OR
ATTEMPT TO VIEW CHILD PORNOGRAPHY**

11. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess and/or attempt to view child pornography:

a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged

in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may possess and maintain hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely completely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child pornography.

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774, 778 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); and *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010), for the principle that the "same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography").

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if a person uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in such a location as the **TARGET LOCATIONS**.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

12. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of a premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

13. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

14. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide

valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called “wireless routers,” which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be “secured” (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or “unsecured” (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator’s network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

PROBABLE CAUSE

15. This ongoing investigation has yielded probable cause that **Edna Lenore Dineen LOPEZ**, of 1528 Mountmor Court, Baltimore, Maryland (MD), has produced sexually explicit videos of minor prepubescent children in her care (henceforth minor victim 1, or MV1, and minor victim 2, or MV2)—and has sold and stored those visual depictions on electronic devices in violation of federal law. **LOPEZ** also performed sex acts on MV1 and/or MV2 while benefiting financially for doing so. **LOPEZ** enticed, provided, advertised, maintained, and solicited MV1 and MV2 to engage in a commercial sex act.

16. Your Affiant is working a child exploitation investigation jointly with the Maryland State Police (“MSP”), Howard County Police Department (“HCPD”), and Baltimore Police

Department (“BPD”). The ongoing investigation has yielded Eugene Edward GOLDEN (“GOLDEN”) possessed child pornography and solicited the production of child pornography.

17. The ongoing investigation has revealed GOLDEN possessed numerous files of child pornography depicting the sexual abuse of infants and toddlers. The investigation has also revealed GOLDEN solicited the production of a number of these child pornography files from various third parties, who appear to have engaged in child sex abuse, including physical abuse of infants and toddlers, at the behest of GOLDEN and in exchange for financial compensation.

18. During an authorized search of GOLDEN’s online Google accounts during the course of the investigation, images of **LOPEZ** with MV1 and MV2 were discovered, as described in detail below.

19. Specifically in July 2022, the Maryland ICAC Task Force assigned NCMEC Cyber Tip #128887022 and eight related cyber-tipline reports (“Associated Cyber Tips”) to the Baltimore Police Department for investigation.

20. NCMEC escalated the Associated Cyber Tips because Cyber Tip #128887022 stated that the referral, “...appears to contain images/videos that appear UNFAMILIAR and may depict NEWLY PRODUCED and/or HOMEMADE CONTENT”. The Associated Cyber Tips indicate that on various dates from 2020-2022, the account user uploaded child pornography to the Google Drive infrastructure.

21. Pursuant to a state search warrant obtained by MSP, Google produced account content containing the Google Drive content for the reported Google account in the NCMEC Cyber Tip. The Google account reported in the Associated Cyber Tips was linked to GOLDEN.

22. Your Affiant reviewed the Google Drive contents and observed over 700 files of commercially available child pornography. Also observed were hundreds of homemade video and image files that depicted adult females sexually abusing children at the behest of GOLDEN. A

review of the apparent homemade files reasonably estimates there are approximately ten (10) to fifteen (15) unique children in the videos solicited by GOLDEN, with at least four (4) to seven (7) adult females who are depicted in the homemade videos.

23. In a number of the homemade videos, the adult females are engaging in the physical and sexual abuse of the child victims. Many of the children appear to be infants or toddlers. In several of the homemade videos, the adult females make sexually charged remarks to “Eugene”, “Gene”, and “Prince”. Additionally, several of the children make remarks to “Mr. Prince” in some of the videos. Your Affiant notes that GOLDEN’s first name is “Eugene”, GOLDEN’s nickname is “Gene”, and GOLDEN’s self-reported moniker is “Prince.”

24. In several of the homemade videos, the adult females specifically tell GOLDEN that he needs to pay them in exchange for their sexual exploitation of their children.

25. On December 1, 2022, the federal grand jury returned an indictment against GOLDEN on charges of 18 U.S.C. 2251(a) (Sexual Exploitation of a Child) and 18 U.S.C. 2252A(a)(5)(B) (Possession of Child Pornography).

IDENTIFICATION OF EDNA LENORE DINEEN LOPEZ

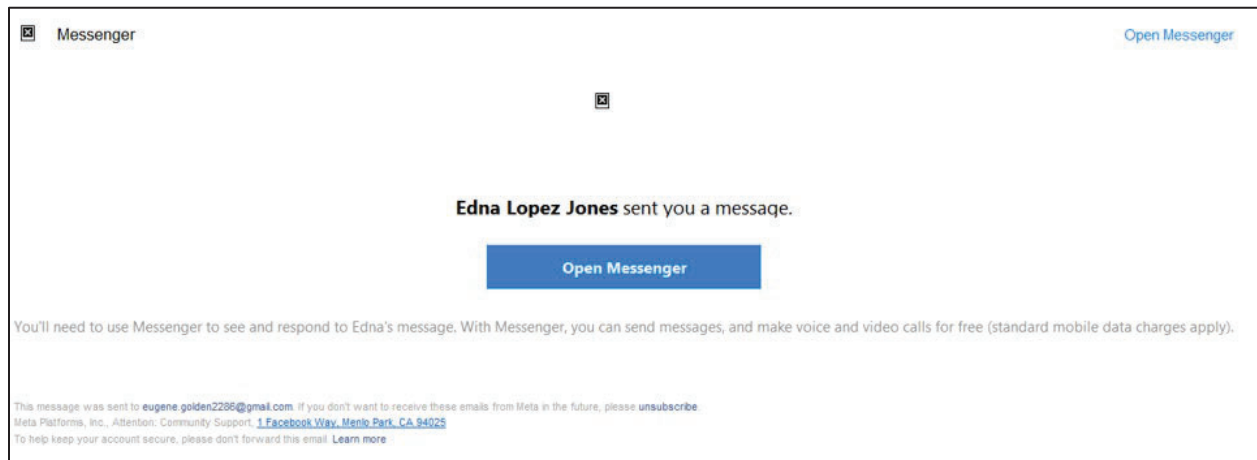
26. Pursuant to the lawfully obtained search warrants and Court Order in this ongoing investigation, Your Affiant has reviewed the account production information that was returned by Apple Inc., Google Inc., Block Inc., as well as the forensic digital analyses conducted on the items seized during the search warrant at GOLDEN’s residence which was executed on November 18, 2022.

27. Your Affiant reviewed the Block Inc. information that was returned associated to GOLDEN’s accounts and accounts associated with transactions made with GOLDEN via CashApp. Specifically, a financial transaction of \$40.00 USD was made between GOLDEN and

an account with username “Edna Lopez” on 2021-06-20 at 21:37:51 UTC. Block Inc. provided the following information for the “Edna Lopez” account:

Active Account Token: C_00c8e1yb8
Identity Verification Name: Edna Lopez
Date of Birth: 10-05-1990
Last Four of Social: 6888
Address History: 1528 Mountmor Court, Baltimore, MD 21217
Display Name History: Edna Lopez, Stacey Flightz, Xavier Jones, Tay Fianc’e, Tay Fianc’ee
Alias History: 4436539530, 2029146258, getmoneyjones11, getmoneyjobes1124, getmoneylopez400, antwanforever1117@gmail.com

28. Upon review of the other account production information received, Your Affiant observed email notifications from Facebook Inc., ranging 11/12/2021 to 03/02/2022, notifying GOLDEN that “Edna Lopez Jones” had sent him a message on Facebook Messenger. Below, Your Affiant has set forth a screenshot of one of the emails GOLDEN received, dated 11/12/2021:



29. Opensource queries revealed the following Facebook account: Edna Lopez Jones. Below, Your Affiant has set forth several screenshots from the Facebook account:



30. Your Affiant observed the following photo caption posted on LOPEZ's Facebook account: "SOOOOOO KNOW IM SUPPOSED TO BE SPREADING HIV DFL....ITS NOTHING TO GO DOWN THE STREET TO THE CLINIC TO GET TESTED TO MAKE ALL U MISERABLE PATHETIC NO LIFE HAVING ASS BITCHES LOOK STUPID...SOOO WITH THAT BEIN SAID LIKE THE PAPER SAYS EDNA LENORE DINEEN LOPEZ IS NEGATIVE FOR HIV".

31. Law enforcement database queries revealed a MVA driver's license for Edna Lenore Dineen **LOPEZ** (hereinafter **LOPEZ**), with DOB 10-05-1990 and SSN ending in -6888.²

² Your Affiant notes this is the same date of birth and last four SSN numbers listed in the CashApp information for "Edna Lopez".

The Driver's License (#L120179506767) was issued on 08-18-2021 and has a listed address for **LOPEZ** as 1528 Mountmor Ct, Baltimore, MD 21217³.

32. Further law enforcement database queries were conducted, which revealed **LOPEZ** had been arrested several times for assault, the most recent being in Baltimore City in 2018. As a result of that arrest, **LOPEZ's** photograph was taken. Below, Your Affiant has set forth **LOPEZ's** Maryland Motor Vehicle Administration (MVA) photo (left), as well as her booking photo from a 2018 arrest (right)⁴:



33. Additional law enforcement database queries revealed that as of September 11, 2022, **LOPEZ** is receiving unemployment benefits. The address listed under **LOPEZ's** contact information for both residential and mailing is 1528 Mountmor Court, Baltimore, MD, 21217. The email account listed is ednalopez58@gmail.com and the phone number listed is 443-469-3431.

34. Queries in the Maryland Judiciary Court system revealed a closed civil case in the District Court for Baltimore City (Case #010100282992013), which lists Edna **LOPEZ** as a Defendant. The case lists a satisfaction date of 07/13/2022. The address listed to **LOPEZ** is 1528 Mountmor Ct, Baltimore, MD 21217.

³ Your Affiant notes this is the same address listed in the CashApp information for "Edna Lopez".

⁴ Your Affiant notes there is a distinct scar on one of the eyebrows of **LOPEZ**.

35. Open-source database queries associate **LOPEZ** with the address of 1528 Mountmor Ct, Baltimore, MD 21217 since approximately January of 2019. The email address ednalopez58@gmail.com is also linked to **LOPEZ** via open-source queries.

36. On December 12, 2022, law enforcement conducted a ruse and knocked on the door of 1528 Mountmor Ct in Baltimore, MD in an attempt to gain information on who lives at the residence. A female, who identified herself as Tiesha Norwood, answered the door. Your Affiant observed the door opened directly into a narrow stairwell, which led to the second level of the building. Ms. Norwood stated she and her cousin, Edna **LOPEZ**, and their minor children, resided at the residence. Ms. Norwood stated her name was on the lease, but her cousin, **LOPEZ**, was really the owner of the residence.

EVIDENCE OF PRODUCTION OF CHILD PORNOGRAPHY



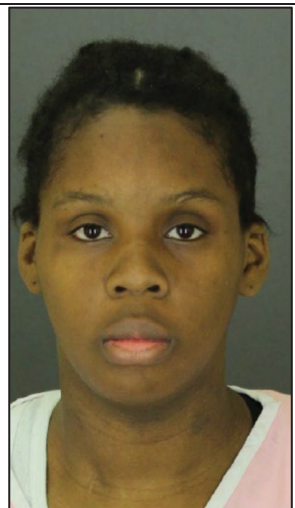
37. As discussed previously in this affidavit, Your Affiant observed several hundred files of apparent homemade files of child pornography involving the sexual abuse of infants and toddlers by adult women in the online accounts of GOLDEN. Your Affiant specifically observed files which contained just **LOPEZ** and no minor children but provided details that allowed other videos to be associated to **LOPEZ** (i.e., clothing, furniture, objects, rooms, etc.). Your Affiant has reviewed these files, and some are described below:

a) **File Name:** 6907184c-f152-4dc4-ae53-c43ed9fe3c14.mp4 (hereinafter **File 6907184c**)

Creation Date: 5/21/2020 1:40:55 AM

Description: This is a color video, one (1) minute and 59 seconds in length, which depicts an adult female, inserting a purple and white vibrator into the mouths of MV1 and MV2. The video begins with both MV1 and MV2 sucking on the two ends of the vibrator that the female is holding. MV1 is only wearing a pair of underwear and MV2 is wearing a pair of blue pants with white stripes on it. The vibration of the sex toy is audible. The adult female tells MV1 and MV2 “Switch” and rotates the vibrator around. The vibrator is then repeatedly penetrated into the mouth of MV1 several times until MV1 states “ouch”. The vibrator is then inserted into the mouth of MV2 while MV1 says, “My turn, my turn!”. The adult female then repeated takes turns inserting the vibrating sex toy into MV1 and MV2’s

mouths. One MV can be heard saying, “It’s going to tickle hurt”. MV1 then states, “My turn” and puts his hand on the vibrating sex toy and it is repeated inserted into his mouth. MV2 can be heard in the background saying “Mommy” and then says something unintelligible. The adult female then continuously proceeds to insert the vibrating sex toy into the mouths of MV1 and MV2 again. MV1 can be heard in the background saying, “Mommy, this is going to hurt.” MV2 moves away from the vibrator and the female states, “Come here”, takes MV2 by the arm, pulls his pants down, and proceeds to slap the vibratory against his butt. MV1 can be heard in the background saying, “Mom, can I get a Lunchable after this?”. The female calls MV1 over and says, “Do the same, come on”. MV1 giggles and says, “It’s going to hurt when you do that”. The female proceeds to pull MV1’s pants down and slap his ass with the vibrating sex toy.

		
<p>Screenshot from File 6907184c, showing a vibrator that was inserted into MV1’s and MV2’s mouths and used to slap their butts (<i>Redacted</i>)</p>	<p>Screenshot from File 6213807a, where the white and purple vibrator used in File 6907184c, is held by LOPEZ with her distinct eyebrow scar⁵ (<i>Redacted</i>)</p>	<p>LOPEZ’s Booking Photo from 2018</p>

b) **File Name:** ef75bca0-7dd8-409f-81fb-453a2ef7f04d.mp4 (hereinafter **File ef75bca0**)

Creation Date: 5/3/2020 9:13:23 PM

Description: This is a color video, 00:55 seconds in length, which depicts LOPEZ and MV2. MV2 is laying on his stomach on the bed, naked from the waist down and wearing a grey t-shirt. LOPEZ is naked from the waist down and wearing a white t-shirt. LOPEZ pulls on MV2 and instructs him to sit up, so he is on his hands and knees and his genitals are exposed. LOPEZ pulls apart MV2’s butt cheeks so his anus is exposed and says, “You

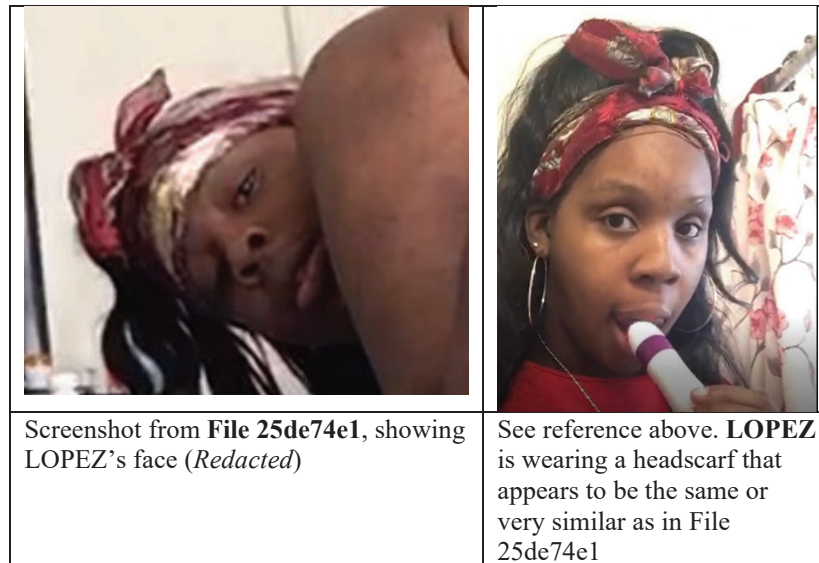
⁵ Your Affiant submits this screenshot from File: 6213807a-73f2-4947-bab1-19ee3006c464.mp4, which has a Exif/Creation Date of 5/20/2020 9:48:17 PM (hereinafter **File 6213807a**), which depicts LOPEZ utilizing a white and purple in color vibrator that is seen in other videos involving MV1 and MV2. Additionally, the headscarf and t-shirt she is wearing and the shower curtain are also observed in other videos involving MV1 and MV2.

want to fuck these asses you pedophile freak bitch. You want us?” LOPEZ then kisses the butt of MV2. MV2 then lays on his stomach and LOPEZ rubs his butt and then exposes her butt and anus to the camera. LOPEZ states, “You freaking pedophile. You child molester bitch. You want to fuck these asses, don’t you?”



c) **File Name:** 25de74e1-7ffd-4737-aca7-56a9c6a22f54.mp4 (hereinafter **File 25de74e1**)
Creation Date: 5/17/2020 8:03:30 PM

Description: This is a color video, 00:27 seconds in length. LOPEZ is naked on a bed with two minor male children, MV1 and MV2. MV1 is naked and on his hands and knees with his butt exposed and in the air. MV1 has a distinctive birthmark on one of his butt cheeks. MV2 is naked from the waist down, wearing a light blue shirt and on his hands and knees on the bed, his butt and genitals exposed and in the air. LOPEZ is on the far right and is completely naked, on her hands and knees with her butt exposed. As LOPEZ looks back at the camera, she says, “Say happy birthday Mr. Prince.” MV1 and MV2 proceed to say, “Happy birthday Mr. Prince!”. MV2 sits up and LOPEZ pushes him back down onto the bed. LOPEZ starts singing “Happy birthday to you” and one of the MVs states, “It’s not my birthday!” MV2 lays down on his stomach on the bed and LOPEZ grabs his leg and states, “Sit up!” as she pulls him back into a position on his hands and knees, then continues to sing “Happy birthday Mr. Prince.” One of the MVs again states “It’s not my birthday”. The video ends with both MV1 and MV2 with their genitals exposed in the air.



d) **File Name:** cf65d5fc-b5f7-4536-bc0f-d3c2df1c35c6.mp4

Creation Date: 5/20/2020 9:48:28 PM

Description: This is a color video, one (1) minute and 56 seconds in length. MV1 is wearing socks but is otherwise completely naked. MV2 is completely naked. MV2 shuffles to the side and MV1 states, "Ma, [name redacted] moving". LOPEZ instructs MV1 and MV2 to turn, resulting in their butts being exposed to the camera. A distinctive birthmark is observed on the butt cheek of MV1.⁶ MV1 bends over at the waist and LOPEZ spreads his butt cheeks to expose his anus. LOPEZ says, "Say hi Mr. Prince". MV1 and MV2 proceed to say, "Hi Mr. Prince!". LOPEZ then states, "Say we love you Mr. Prince." MV1 and MV2 proceed to say, "We love you Mr. Prince!". LOPEZ then says, "We got some butt for you Mr. Prince." MV1 and MV2 proceed to say, "I got some butt for you Mr. Prince!". LOPEZ then states, "Say don't you like butt?", to which MV1 and MV2 say, "Don't you like butt?" MV1 is bent over, exposing his ass. LOPEZ states, "Say, do you like my butt?". The MVs then say, "Do you like my butt?". LOPEZ instructs, "Say booty booty everywhere. Ding ding everywhere". The MVs say "Booty booty everywhere. Ding ding everywhere" as they dance around. LOPEZ then instructs the MVs to shake their bootys and then smack their butts. The MVs comply. The MVs continue to dance around and smack their own butts. At one point, LOPEZ refers to MV2 as "[name redacted]". LOPEZ says, "Bend over. Twerk", to which MV1 responds, "No mom, I'm a boy!".

⁶ Your Affiant notes this is the same birthmark observed and mentioned in file description c.

38. The files identified and associated to **LOPEZ** from the Google Drive linked to GOLDEN's accounts, some of which Your Affiant has discussed above, reflect "creation dates" between 05/02/2020 and 05/07/2021 in their metadata.

UNLOCKING BIOMETRICALLY SECURED DEVICES

39. Unlocking the device(s) with biometric features. The warrant I am applying for would permit law enforcement to compel **LOPEZ** to unlock (1) any device on **LOPEZ'S** and person; and (2) any device in **LOPEZ's** residence reasonably believed to be owned, used, or accessed by **LOPEZ**; I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera

detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device (such as an iPhone) has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

40. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **LOPEZ** to the fingerprint scanner of the seized device(s); (2) hold the device(s) in front of the face of **LOPEZ** to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of **LOPEZ** and activate the iris recognition feature for the purpose of attempting to unlock the device(s), and attempting the access data contained in the device, in order to search the contents as authorized by this warrant.

CONCLUSION

41. Based on the above information, I respectfully submit there is probable cause to believe that Edna Lenore Dineen **LOPEZ** has committed violations of 18 U.S.C. 2251(a)(Sexual Exploitation of Children); 18 U.S.C. 2252A(a)(2) Distribution of Child Pornography; and 18 U.S.C. 1591 (a), (b)(1)(Sex Trafficking of Children) from in or about May 1, 2020, to May 31, 2021. Based on the activity of **LOPEZ** detailed above, as well as my training and experience, I believe that the **LOPEZ** engaged in sex trafficking of children, produced child pornography and distributed child pornography. I respectfully request that this Court issue an arrest warrant for Edna Lenore Dineen **LOPEZ**.

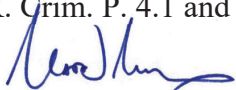
42. Further, I respectfully submit that that there is probable cause to believe that the **TARGET OFFENSES** have been violated, and that the property, evidence, fruits, and instrumentalities of these offenses listed in Attachment B-1, which are incorporated herein by reference, are located in the **TARGET LOCATIONS**, further described in Attachments A-1 and A-2.

43. Therefore, based upon the foregoing, I respectfully request that this Court issue search warrants for the **TARGET LOCATIONS**, more particularly described in Attachments A-1, A-2, authorizing the seizure of the items described in Attachment B-1.



Rachal M. Torg
Special Agent
Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 14th day of December 2022.



HONORABLE MATTHEW J. MADDOX
UNITED STATES MAGISTRATE JUDGE